COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department on its own motion, pursuant to G.L. c.159 § § 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	)	**D.T.E. 02-8**

PANEL TESTIMONY OF VERIZON MASSACHUSETTS

Members of the Panel:

Lawrence R. Craft
Francesco S. Mattera
Lynelle Reney
Peter Shepherd

April 5, 2002

PURPOSE OF TESTIMONY

Q. What is the purpose of this testimony?

A. In this testimony, Verizon Massachusetts ("Verizon MA") addresses issues raised by the Department's *Order to Investigate* issued January 24, 2002, in this proceeding, regarding the Company's existing collocation security policies established as a result of the Department's findings in D.T.E. 98-57, Phase I.[1] *Order to Investigate*, at 1. As stated in its *Order to Investigate*, the Department's intent is to review its prior findings with respect to access by personnel of other carriers to Verizon's central offices and other facilities, and to assess whether the security measures adequately protect the telecommunications network and facilities in light of heightened security concerns following the September 11, 2001, terrorist attacks in New York City and Washington, D.C.. *Order to Investigate*, at 1. Specifically, the Department's investigation will include, but not be limited to, an examination of the following issues: (1) the extent and nature of appropriate access by personnel of other carriers to Verizon's central offices and other facilities [*e.g.*, remote terminals] for accessing collocation sites; (2) whether cageless collocation arrangements remain an acceptable security risk; (3) the adequacy of security measures implemented in Verizon's central offices

[1] *See* D.T.E. 98-57, Phase I, *Order*, at 24-39, 59-62 (March 24, 2000); D.T.E. 98-57, Phase I, *Reconsideration Order*, at 6-16, 66 (September 7, 2000); D.T.E. 98-57, Phase I, *Phase I-B Order*, at 16-20 (May 24, 2001).

and other facilities, focusing on preventive, rather than "after-the-fact," measures; and (4) any other related security issues. *Id.* at 7.

Verizon MA's testimony examines the various currently available collocation arrangements and the applicable security measures for central offices ("CO") and other collocated facilities. Based on the increased potential for network harm resulting from the presence of physical collocation and Verizon's experience with security breaches in Massachusetts and elsewhere, the Company concludes that current collocation security measures must be adequately strengthened "to safeguard the telecommunications networks from tampering," and thereby "ensure that reliable service to competing telecommunications service providers, businesses, and residents of the Commonwealth is not unreasonably at risk" in a post-September 11th world, as the Department suggests. *Id.* at 2.

Verizon MA recognizes that the "reasonable" security measures permitted by the Federal Communications Commission ("FCC"), such as cameras, electronic card readers, or badges with computerized tracking systems,[2] can provide detection for security breaches "after the fact," and may even *deter* them in some cases. However, deploying such equipment is not enough for Verizon MA to *prevent* unauthorized access to its COs or to unsecured areas within the COs. Unauthorized CO access can also jeopardize Verizon MA's ability to protect even

[2] *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Fourth Report and Order, CC Docket No. 98-147, FCC 01-204 (rel. Aug. 8, 2001) ("*FCC Remand Order*"), on remand from the U.S. Court of Appeals' decision in *GTE Service Corporation v. FCC*, 205 F.3d 416 (D.C. Cir. 2000) ("*GTE Service Corporation*").

its "secured" space *within* the restricted areas of the CO. Accordingly, the Department should allow Verizon MA to take the necessary *pro-active* steps to prevent damage to the critical telecommunications infrastructure that can occur either accidentally or intentionally when carriers have access to COs in a physically collocated environment.

Without such pro-active security measures, Verizon's network, as well as the facilities and equipment of collocated carriers, remain exposed to an increased risk of harm. Although pro-active security measures (*e.g.*, separate space and separate entrances) cannot totally eliminate security risks, they can substantially minimize them and, thus, better protect and preserve the network in a physically collocated environment so that Verizon MA and other service providers can maintain uninterrupted service for their end-user customers, which include state and federal government installations and business that are critical to the public welfare.

Q. Please explain briefly Verizon MA's proposed security measures at collocated COs.

A. Verizon MA believes that the most effective means of ensuring network safety and reliability is to eliminate physical collocation entirely in all its COs, converting existing physical collocation arrangements to virtual and requiring that all future collocation arrangements be virtual only. However, the Company recognizes that this is not a practical solution from a legal and regulatory

perspective at this time. Therefore, Verizon MA proposes that the following *pro-active* collocation security measures be adopted based upon the potential for network harm and Verizon's experience with security breaches in Massachusetts and elsewhere.

They are: (1) the establishment of separate space with separate entrances and/or pathways for all forms of physical collocation (*i.e.*, caged and cageless) to secure and segregate collocators' equipment from Verizon MA's equipment and no commingling of collocators' equipment in the same rooms as Verizon MA's equipment without some reasonable means of physical separation (*e.g.*, partitioning) and secured access; (2) the relocation of existing *unsecured* cageless collocation arrangements to a secured and segregated area of the CO or the conversion of such arrangements to virtual collocation where secured CO space is unavailable; (3) the provision of reasonable access to shared facilities (*e.g.*, temporary staging areas, elevators, loading docks, restrooms, etc.)[3] that are located outside the secured and segregated collocators' space either by partitioning Verizon MA's equipment, if feasible, or through the use of escorts at the collocated carrier's expense; (4) the requirement to provide virtual collocation and/or escorts at physically collocated remote terminal ("RT") sites; and (5) the development of more stringent measures in critical, "high" security risk COs, *i.e.*,

[3] *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, First Report and Order and Further Notice of Proposed Rulemaking, CC Docket No. 98-147, 14 FCC Rcd 4761, at ¶ 49 (March 31, 1999) ("*FCC Advanced Services Order*") (requiring that collocated carriers be allowed "reasonable access to basic facilities" while at the incumbent LEC's premises).

classify such COs as "virtual collocation only" sites. In that regard, Verizon MA would propose to work with the Department in determining which COs would be so classified, and to convert existing physical collocation arrangements to virtual collocation in those designated COs, subject to Department approval.

Notwithstanding the above proposed pro-active security measures, Verizon MA also plans to deploy and indeed enhance the use of various security devices (*e.g.*, electronic card reader systems, cameras, etc.), as appropriate, based on the needs of the particular CO.[4] Verizon MA also plans to implement an in-depth, pre-screening of collocated carrier personnel designated to access physical collocation arrangement in its COs as a requirement of providing identification badges. This is consistent with Verizon's more stringent pre-screening and background checks for its employees and vendors that are being adopted as part of its nationwide efforts to enhance security in its COs since September 11th.

Verizon MA believes that these proposed security measures and enhancements are necessary because of the present network architecture and configuration of equipment and facilities in Verizon MA's COs and RTs. Such measures will better protect the telecommunications network from harm in today's environment, as well as maximize safety and security for employees and agents of Verizon and

[4] For example, Verizon plans to expand the number of COs equipped with electronic card reader systems ("CRAS"), in lieu of locked key access.

collocated carriers.[5] Strengthened security procedures will also reduce the degree of risk to Verizon MA's facilities, and further enable the Company to provide reliable service to end user and carrier customers alike in Massachusetts.

WITNESS PANEL

Q. Please identify the name and business address of the individual panel members testifying on behalf of Verizon MA in this collocation security investigation.

A. The members of this panel, in alphabetical order, are: Mr. Lawrence R. Craft, Mr. Francesco S. Mattera, and Ms. Lynelle Reney. Mr. Craft's business address is 1320 North Courthouse Road, Arlington, Virginia; Mr. Mattera's business address is 125 Circular Avenue, Paoli, Pennsylvania; and Ms. Reney's and Mr. Shpeherd's business address is 125 High Street, Boston, Massachusetts.

Q. Please describe the current position, educational background and professional experience of each panel member.

A. **Mr. Lawrence R. Craft** is a Manager in Verizon's Security Department, and is responsible for Verizon East's (*i.e.*, former Bell Atlantic jurisdictions') Physical Security/Access Control function, which establishes Corporate physical security

[5] In addition, to protect the collocated carrier's equipment in a physical collocation environment, Verizon MA may offers carriers the option of requesting *covered* cages, at their own expense, in traditional physical collocation arrangements. Collocated carriers also already have the option of cabinetizing their equipment as an added security measure with cageless collocation. However, it is not technically, operationally or economically feasible for Verizon MA to partition all of its CO equipment to protect the network from harm because of the manner in which the Company' network (*i.e.*, CO equipment) configuration has evolved over time.

standards, physical security planning, and daily security operations for most of the Verizon East area. Since 1996, he has held various security assignments in International Security, Physical Security, and Access Control, and currently acts as a liaison with certain governmental organizations in his capacity as Verizon's Corporate Security Control Officer for the U.S. Government Industrial Security Program. Mr. Craft has 24 years experience in telecommunications, as an employee of the Chesapeake and Potomac ("C&P") Telephone Company of West Virginia, Bell Atlantic and Verizon. During that time, he has held management positions in various departments, including Supply Management, Motor Vehicle Management, Real Estate, Administration, Finance and Security. Mr. Craft is a retired United States Army Reservist with 20 years honorable service. He earned his Bachelor's degree from West Virginia University, with post-graduate studies toward a Masters of International Administration at Central Michigan University.

Mr. Francesco S. Mattera has held his current position as a Director of Network Operations since July 2000. In that capacity, he is responsible for deploying new technology architectures and developing the associated processes for Verizon's Network Operations Department. Mr. Mattera earned both a Bachelor of Science degree and a Masters in Business Administration ("MBA") from Drexel University. He has 15 years of experience in Bell Atlantic and Verizon Communications. During that time, Mr. Mattera has held a variety of positions of increasing responsibility in Engineering, International, and Network Operations.

Ms. Lynelle Reney is Director of Collocation for Verizon East. In her current position, she is responsible for overseeing all functions related to collocation application receipt and processing, including issuing acknowledgment letters, cost/schedule letters and notifications to competitive local exchange carriers ("CLECs"), and for overseeing the billing of all collocation arrangements and the Collocation Care Center ("CCC"), which provides ongoing support to collocators, including providing and managing ID and access cards.. Ms. Reney has 17 years of experience in New England Telephone, NYNEX, Bell Atlantic and Verizon. During that time, she has been employed in various departments, including Real Estate, Equipment Installation, and Corporate Services. Ms. Reney earned both a Bachelor's degree and MBA from the University of Rhode Island. She has testified before the Pennsylvania Public Utility Commission in Docket No. P-00001852 (a dispute resolution proceeding regarding the provisioning and billing of DC power), and has submitted direct written testimony as a member of Verizon's witness panel in Massachusetts in D.T.E. 98-57 III and D.T.E. 01-39.

Mr. Peter Shepherd is Director - Regulatory for Verizon. He has 32 years of experience in New England Telephone, NYNEX, Bell Atlantic and Verizon. During his employment, Mr. Shepherd has held various positions in the Network, Marketing and Regulatory Departments. His responsibilities in those various positions include Central Office operations, Independent Telephone Company business relations and joint network planning, access services product management and pricing, service costs and regulatory matters dealing with rate

design, pricing rules, and regulatory structure in Maine, Massachusetts, New Hampshire, Rhode Island and Vermont. Mr. Shepherd holds a Bachelor of Science degree and an MBA from Babson College. He has previously testified in Maine, Massachusetts, New Hampshire, Rhode Island and Vermont on alternative forms of regulation, rate case, access charges, rates & costs, price floors and special contracts.

CURRENT SECURITY MEASURES FOR COLLOCATION ARRANGEMENTS

Q. Please identify the different forms of collocation arrangements currently available in Massachusetts.

A. Verizon MA offers the following types of collocation arrangements: (1) traditional "caged" physical collocation, (2) secured collocation open environment ("SCOPE"); (3) cageless collocation open environment ("CCOE"); (4) virtual collocation; (5) adjacent collocation; (6) shared collocation; (7) microwave collocation; and (8) collocation at remote terminal equipment enclosures ("CRTEE"). Currently, Verizon MA provides 536 traditional "caged" physical collocation arrangements, 385 SCOPE, 27 CCOE, four virtual collocation arrangements, and one shared collocation arrangement located in a total of 169 COs in Massachusetts.[6]

[6] Currently, Verizon MA has not provisioned any CRTEE, adjacent or microwave collocation arrangements. However, the Company is currently processing one customer's physical collocation application for microwave entrance facilities in Massachusetts.

Q. Please describe briefly the different characteristics of Verizon MA's various collocation arrangements.

A. The traditional "caged" physical collocation arrangement allows a CLEC to place its equipment in a wire mesh enclosure or cage – available in varying standard sizes (*e.g.*, 25, 100 or 300 square feet) – within a segregated and secured, environmentally conditioned area of Verizon MA's CO. By contrast, SCOPE and CCOE are forms of physical collocation that allow the placement of CLEC equipment in single bay increments[7] in Verizon's CO without requiring an individual cage or wire mesh enclosure. While SCOPE arrangements are placed in the same segregated and secured, environmentally conditioned area used for traditional "caged" physical collocation, CCOE arrangements may not require the construction of a separate collocation area, *e.g.*, a separate room or isolated space segregated from Verizon's own network equipment. Rather, due to space limitations, CCOE may be located in non-secured, non-separated space within Verizon's CO premises.

Unlike physical collocation, a virtual collocation arrangement does not require Verizon MA to assign a portion of the floor space in the CO to the collocated carrier for its exclusive use to install, operate and maintain its own equipment. Rather, the CLEC leases its equipment to Verizon MA to install, maintain,

[7] "Single-bay increments" means that a CLEC can purchase space in increments small enough to collocate a single rack, or bay, of equipment.

upgrade and repair on Verizon's premises under the direction - and for the benefit – of the CLEC.

While a CLEC cannot directly access the collocated equipment, nor enter Verizon's premises, a CLEC can, however, establish comparable systems used in a physical collocation environment to access remotely its virtually collocated equipment for monitoring, provisioning and testing purposes. Virtual collocation is provided "where physical collocation is not practical for technical reasons or because of space limitations" in a particular CO, and is also available as an option for a CLEC in *any* CO.[8] 47 U.S. §251(c)(6).

Adjacent collocation is offered when there is no space available within Verizon's CO for physical collocation. Under adjacent collocation, the CLEC may construct or otherwise procure controlled environmental vaults ("CEV") or similar adjacent structures, where technically feasible, using Verizon approved vendors.

Shared collocation enables a CLEC to share its "caged" physical collocation space with other CLECs under a subleasing arrangement. Microwave collocation enables CLECs to interconnect their collocation equipment with Verizon's

[8] Security and network reliability issues are valid factors to consider in determining whether physical collocation is technically feasible. *See e.g.*, *In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996,* CC Docket No. 96-98, FCC 96-325, *First Order and Report* (rel. August 1996), ¶ 203 ("*Local Competition Order*"); *see also* CC Docket Nos. 01-338, 96-98, 98-147, FCC 01-361, *Notice of Proposed Rulemaking* (rel. December 20, 2001), ¶ 33 .

facilities using microwave antennae on the rooftop of Verizon MA's COs. Microwave facilities provide an alternative transport option to fiber facilities to a collocation arrangement.

Finally, CRTEE provide arrangements in which CLEC equipment can be placed in Telephone Company remote terminal equipment enclosures ("RTEEs"). CRTEE can be provided on either a physical or virtual arrangement basis. RTEEs include controlled environment vaults, huts, cabinets and remote terminals in buildings or similar structures owned or leased by Verizon MA to house the Company's network facilities.

Q. What security measures may Verizon MA currently apply under the various collocation arrangements?

A. In accordance with 47 C.F.R. §51.323(i), Verizon may require reasonable security arrangements to protect its own equipment and ensure network reliability.[9] The security arrangements imposed may only be as stringent as those it applies to itself or its authorized vendors. Verizon must also allow CLECs 24 hour per day, seven day per week access to their collocated equipment without the requirement of a security escort.

Verizon MA may adopt reasonable security measures for its collocation arrangements, including those set forth in 47 C.F.R. §51.323(i): (1) installing

[9] *FCC Advanced Services Order*, at ¶46 (finding that the ILEC "may take reasonable steps to protect its own equipment"), cited favorably in *GTE Service Corporation*, 205 F.3d at 426.

security cameras or monitoring systems; (2) requiring CLEC personnel's use of badges with computerized tracking systems; (3) requiring CLEC personnel to undergo the same or equivalent level of security training as Verizon's own employees or authorized vendors, provided that the CLEC is not required to receive such training solely from Verizon; (4) restricting physical collocation space to space that is physically separated from space housing Verizon's equipment;[10] and (5) requiring access through a central or separate entrance provided that Verizon affiliates and subsidiaries have the same requirement.[11] In providing reasonable security arrangements, Verizon MA may require CLECs to pay only for the least expensive, effective security option that is viable for the physical collocation space assigned.

Q. How do the Department's findings in D.T.E. 98-57, Phase I compare with the FCC's requirements in 47 C.F.R. §51.323?

---

[10] This type of security measure is subject to the following conditions: (i) either legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant such separation; (ii) any physical collocation space assigned to an affiliate or subsidiary of the incumbent LEC is separated from space housing the incumbent LEC's equipment; (iii) the separated space will be available in the same time frame as, or a shorter time frame than, non-separated space; (iv) the cost of the separated space to the requesting carrier will not be materially higher than the cost of non-separated space; and (v) the separated space is comparable, from a technical and engineering standpoint, to non-separated space. 47 C.F.R. §51.323(i)(4).

[11] The following conditions must be met to apply this security measure: (i) construction of a separate entrance is technically feasible; (ii) either legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns, warrant such separation; (iii) construction of a separate entrance will not artificially delay collocation provisioning; and (iv) construction of a separate entrance will not materially increase the requesting carrier's costs. 47 C.F.R. §51.323(i)(4).

A. The Department's findings on collocation security measures in its D.T.E. 98-57, Phase I, Orders are generally consistent with the FCC's requirements[12] under 47 C.F.R.. For example, the Department rejected an escort requirement for physical collocation[13] because it would "unduly impede a CLEC's access to its equipment and increase costs." *Reconsideration Order*, at 13; *see also Phase I-B Order*, at 19. The only exception is that Verizon may provide escorts, at no cost to the CLECs, prior to implementation of permanent security measures at a CO, in certain limited instances. *Order*, at 28.

In clarifying the issue of CLEC access beyond their collocation arrangement, the Department stated that Verizon MA may prohibit a CLEC from access to any area within the CO where the CLEC does not have any equipment located. The Department further clarified that it does not intend to prohibit Verizon from deploying an efficient mix of security measures within a CO, but rather to prevent the deployment of duplicative security measures that would increase the costs of collocation without providing a necessary security benefit. *Reconsideration*

---

[12] This includes the use of security cameras, electronic card readers, and badge tracking systems. *Order*, at 27. Other security measures permitted by the Department include: (1) a 30-minute prior notification by the CLEC to Verizon before dispatching a technician is sufficient for both manned and unmanned central offices; and (2) the designation of a specific (even separate) entrance for CLEC use during work stoppages. *Id.* at 32, 39.

[13] Verizon MA, however, disagrees with the Department's conclusion that the existing FCC rules prohibit escorts for CRTEE. *Phase I-B Order*, at 19. The issue of requiring escorted access to CEVs and huts is currently under review at the FCC. *See e.g., Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Order on Reconsideration and Second Further Notice of Proposed Rulemaking in CC Docket No. 98-147 and Fifth Further Notice of Proposed Rulemaking in CC Docket No, 96-98, FCC 00-297, at ¶ 104 (rel. Aug. 10, 2000) ("*FCC Reconsideration Order*").

Order, at 15. Finally, the Department issued a stay on its earlier directives regarding the construction of separate collocation rooms, the commingling of equipment, and conversions from virtual to cageless collocation, pending a final decision by the FCC on those issues. *Reconsideration Order*, at 15.

Q. What is the status of the FCC's collocation security provisions under 47 C.F.R. 51.323?

A. Those provisions, along with other collocation issues decided in the *FCC Remand Order*, issued August 8, 2001, are pending review before the U.S. Court of Appeals for the D.C. Circuit (the "Court") in Nos. 01-1371 and 01-1379. The basis for that appeal is that, on remand from the Court's decision in *GTE Service Corporation*, the FCC re-imposed highly intrusive space allocation and access requirements for "physical collocation" on incumbent local exchange carriers ("ILEC") that grant unwarranted rights to CLECs to control the specific location of their equipment within the ILEC's premises and to access that collocated equipment.[14] The petitioners[15] argue, *inter alia*, that in doing so, the *FCC Remand Order* - which was released one month before the events of September 11th - effectively establishes a default rule that forecloses ILECs from requiring

[14] The Court in *GTE Service Corporation* found "nothing in §251(c)(6)" to support the FCC's requirement "that competitors, over the objection of LEC property owners, are free to pick and choose preferred space on the LEC's premises, subject only to technical feasibility." 205 F.3d at 426. Nor did it find authority for the FCC to prohibit ILECs from requiring competitors to place their equipment in segregated rooms or floors or to use separate entrances. *Id.*

[15] The petitioners to this appeal include the Verizon Telephone Companies, BellSouth Corporation and SBC Communications, Inc.

segregated space and separate entrances, thereby unduly interfering with the ILEC's fundamental right to manage effectively the use of its property and its obligations to protect the security of its telecommunications infrastructure and the safety of its employees.

Notwithstanding the FCC conditions set forth in 47 C.F.R. § 51.323, which are the subject of this appellate review, Verizon MA requests that the Department permit the Company to establish the proposed *pro-active* security procedures that would secure and segregate – and, therefore, better protect - the telecommunications network infrastructure from harm – both unintentional and deliberate. These are reasonable and necessary security measures, particularly in light of legitimately heightened security concerns resulting from the events of September 11th. Accordingly, the Department should join with Verizon to ensure that additional security measures can be implemented, and seek appropriate changes to FCC rules, if necessary.

Q. Please identify the types of security methods currently used by Verizon MA at collocated sites.

A. Verizon MA uses the following security methods for providing CLECs' access to their collocated space, as well as shared facilities(*e.g.*, access to loading docks, temporary staging areas and restrooms), within Verizon's CO: (1) non-Verizon employee collocation identification (ID) cards; (2) electronic card reader access systems; (3) key controlled access systems; (4) directional signage and floor

markings (*e.g.*, floor tape); and/or (5) access through guarded entries. In addition, Verizon MA deploys security cameras, *i.e.*, Closed Circuit Television ("CCTV"), in COs with unsecured CCOE arrangements or where access to shared facilities is only available by means of unsecured open passage through Verizon MA's equipment areas. A detailed description of Verizon MA's administration and practices for these various security devices is appended as Attachment 1 to this testimony.

CLECs and their authorized employees, agents and contractors who have a legitimate need to access the CLEC's own physical collocation arrangement must abide by all Verizon security and safety practices while on Verizon's premises. Verizon's current practices are available to CLECs on the Company's website at http://128.11.40.241/east/wholesale/html/pdfs/RSECOL00.pdf. Violators are subject to removal and termination of all access privileges.

Q. Does Verizon MA consider its current collocation security measures to provide adequate protection from harm to its network at collocation sites?

A. No. Although Verizon MA has always had security concerns with physical collocation, those concerns are exacerbated in the current world environment.[16]

[16] *See e.g.*, Michael K. Powell, Chairman, FCC, *Digital Broadband Migration Part II*, at 11, Remarks at FCC Press Conference (Oct. 23, 2001) ("Securing Our Nation's Communications Infrastructure" is a "Principal Objective" of "Homeland Security"), *at* www.fcc.gov/Speeches/Powell/2001/spmkp109.pdf; *see also* Young & Berman, *Exposed Wires: Trade Center Attack Shows Vulnerability of Telecom Network*, Wall St. J., Oct. 19, 2001. These materials are appended as Attachment 2 to this testimony.

As recognized by the Department in initiating this investigation, because of recent events, there is a need to reexamine and strengthen existing security practices and procedures relating to CLEC access to collocated sites. While the current security methods that Verizon is permitted to use to protect its network at collocated sites may deter some security violations, they primarily enable Verizon MA to detect and respond to security violations "after-the-fact." Moreover, the current security tracking measures simply will not prevent some individuals from causing either intentional or unintentional damage to Verizon MA's network. Verizon MA, therefore, proposes to take more pro-active steps to protect its infrastructure — the integrity of which is critical for the reliable, uninterrupted provision of voice, data, and emergency telecommunications services to the public. Without these additional security measures, the potential personal and financial loss to consumers and businesses, including other carriers and governmental entities, could be substantial and far-reaching.

Q. Please explain why security cameras alone are not an effective means of monitoring and preventing accidents or damage to Verizon MA's network in the CO.

A. The use of cameras *alone* is neither an effective nor efficient pro-active security method. First, multiple cameras positioned in many locations throughout a CO would be required to capture all potential activity – and even then it would be virtually impossible to capture *every* angle in a CO to prevent or even sufficiently

deter potentially harmful activity.[17] Second, Verizon MA primarily uses digital cameras, not analog cameras that provide real-time monitoring. Third, the number of individuals required per CO to observe the video screens with real-time monitoring would be substantial and extremely costly. This is compounded by the need to monitor many COs.

For example, since CLECs can access COs 24 hours a day, seven days a week, a minimum of four guards per collocated CO (or one per shift) would be required to provide real-time monitoring. Moreover, to prevent incidents from occurring, the posted guard must be sufficiently knowledgeable to identify suspicious activities, and adequately trained to intervene if an illegal or disruptive action is observed. Accordingly, although cameras may be useful to record events – and even deter crimes in certain cases, cameras *alone* are not enough as a pro-active security measure to prevent unauthorized access to a physically collocated CO environment.

Q. Please explain why electronic card reader access systems alone are not an effective pro-active security method.

[17] It is particularly difficult for cameras to cover reasonably every square inch of a physical facility in a CO environment, where many obstructions (*e.g.*, tall equipment bays and line-ups, ladders, and bulky equipment) may block the camera's view and make it impossible to determine precisely what an individual is doing. Indeed, even if enough cameras were installed to capture *every* angle in a CO, the quality and/or distance of the picture would simply not be sufficient to capture an individual's precise movements, and may not even be sufficient to determine the exact piece of equipment being worked on or tampered with.

A. Although electronic access card readers may provide some level of security to deter and detect security breaches when combined with other methods, such as cameras or partitions, they alone are not enough to prevent accidents or damage to the network infrastructure. While security access cards are intended to prevent unauthorized personnel from accessing certain sections of the CO and to provide Verizon with a record of who enters its offices, they do not necessarily and conclusively identify the "user."

For example, Verizon is aware of instances where CLECs have not reported lost access cards or returned cards given to former employees and representatives. Verizon is also aware of CLEC personnel or agents using cards belonging to others.[18] The ability to "share" access cards renders them useless at determining responsibility for damage to the network. Moreover, even if access cards are used properly, they may only provide Verizon with a witness or suspect for accidents or intentional bad acts. Thus, because the negligent use or misappropriation of access cards is undetected until "after-the-fact," access cards may have limited use as either a practical or effective pro-active security measure.

In addition, card readers do not show when an individual leaves a CO, thus making it impossible to determine the duration of an individual's stay or if he/she

[18] For example, there have been incidents where CLEC employees have entered the CO without an authorized identification badge, but with another CLEC employee's electronic access card. Moreover, at many Verizon MA COs, secondary exits are not monitored since they serve solely as exits. Such breaches, however, often go undetected and unpunished because Verizon does not have the same recourse against CLEC violators as it does with its own employees or vendors (*i.e.*, Verizon cannot discipline a CLEC violator or terminate his/her employment).

was in the office when a security breach occurred. Nor do card readers indicate when individuals "tailgate" other CLECs or vendors, *i.e.*, walk in behind them without swiping an access card across the reader. In the future, CLEC personnel could be compromised by giving CO access to an outside entity that is not authorized to enter Verizon's CO and does not understand the disruption or damage that could be done to by certain activities, which could affect critical facilities. Indeed, card reader systems can only be fully effective when used in conjunction with physical barriers or partitions that separate CLEC and Verizon MA equipment space and prevent unauthorized access to or through Verizon MA's equipment areas in the CO.

Q. Has Verizon MA experienced serious security violations in Massachusetts to warrant the adoption of more stringent security measures?

A. While Verizon has fortunately not experienced egregious and harmful security violations in Massachusetts, there have been serious violations elsewhere, some of which have resulted in service interruptions for many end user and carrier customers. Whether the result of carelessness or blatant disregard for existing security rules, these CLEC violations raise legitimate security concerns and presage what could occur anytime in Massachusetts under the current collocation security procedures.

For example, across the country, Verizon has documented such violations as unauthorized entry into CO areas outside of the CLEC's collocated equipment

space; theft and vandalism of CLEC equipment resulting from unauthorized access to a CLEC's cage, theft and vandalism of Verizon equipment in secured and unsecured areas of the CO; cables cut on frames; CLEC entry without an authorized identification badge or electronic access card; CLEC entry with unauthorized use of another's identification badge or electronic access card; doors propped open or locks taped; such acts of vandalism as broken locks on doors or collocation cages, card readers destroyed, or power systems disabled; unauthorized CLEC testing on Verizon's side of the equipment; evidence of drug use on the CO premises; and other improper conduct..[19]

The numerous different collocators, their employees and agents increase the sheer number of unfamiliar personnel accessing the CO. This, in turn, vastly increases the probability of accidents, mistakes, and outright wrongdoing and, therefore, the exposure to financial harm and damage to Verizon's network. CLEC personnel may also have less incentive to exercise care with Verizon's or other collocated carriers' equipment, or may be less trained or less familiar with the CO environment and the potential incidental harm to the various types of CO equipment.

[19] Verizon is aware of at least one instance in Washington state where a security violation, [*e.g.*, the CLEC entered Verizon's Battery Distribution Fuse Bay ("BDFB") in a secured area to turn up power in its collocated equipment) caused a service outage in a remote switch, interrupting service to approximately 9,000 customers. In addition, Verizon has experienced cases where CLEC personnel have broken into locked power rooms in the Company's CO in an attempt to work on power distribution equipment (*e.g.*, the power distribution panel), creating a serious safety risk as well as the potential for widespread service interruptions. Fortunately, these failed attempts to

Verizon MA cannot require security escorts for CLECs to access their collocated equipment, which is permitted 24 hours a day, seven days a week. This unrestricted access, combined with unseparated space and/or commingled equipment, creates security risks that increase the likelihood of accidents – whether inadvertent or intentional – and the threat of sabotage. Accordingly, additional security procedures must be adopted to protect Verizon's network.

VERIZON MA'S PROPOSED COLLOCATION SECURITY PLAN

Q. What additional security measures does Verizon MA propose in this proceeding for its collocated sites in Massachusetts?

A. Verizon MA proposes the following: (1) establishing, for all forms of physical collocation (caged and cageless) separate space (*e.g.*, separate rooms, floors, entrances and/or pathways to such areas) that secures and segregates collocators' equipment from Verizon MA's network facilities and prevents the commingling of collocators' equipment in the same areas as Verizon MA's equipment on an unseparated or unsecured basis; (2) relocating existing *unsecured* CCOE arrangements to secured, separated areas, where space permits, or otherwise converting them to virtual collocation arrangements; (3) providing CLECs with reasonable access to shared facilitiesoutside the secured and segregated collocation space where partitioning of Verizon MA's equipment is feasible; (4)

---

work on Verizon's power equipment did not result in injury to the workers or cause damage to the network.

providing either virtual collocation and/or escorts for CRTEE arrangements; and (5) converting existing physical collocation arrangements to virtual collocation in selected, highly sensitive security risk COs. These proposed security measures are appropriate, reasonable, in the public interest, and necessary to ensure the security, reliability and safety of Verizon MA's telecommunications infrastructure in today's environment based on the Company's network architecture.

Q. Please briefly describe Verizon MA's network architecture.

A. Verizon MA provides the backbone platform for data, voice, and long distance services for its end-user and carrier customers. Generally Verizon MA's network consists of three basic components: (1) network access or loop facilities; (2) central office buildings that contain switching, transmission, power plant and other support system equipment; and (3) interoffice transmission facilities. A diagram of this basic network design and a more detailed description of the various network components are appended to this testimony as Attachment 3.

As described in Attachment 3, the CO is the "hub" where network access lines and interoffice facilities are combined to connect with other facilities to provide telecommunications services to residence and business customers, including governmental, financial and public safety organizations, as well as to carrier customers that interconnect their networks to Verizon or subscribe to its wholesale or retail services. All of those customers depend on the reliability of Verizon MA's telecommunications network. Moreover, based on current

technology and network configurations, any inadvertent or intentional damage in a given CO may impair multiple end offices with potentially significant service-affecting consequences, including but not limited to the interruption of public safety or emergency services.

At the time that COs were originally built, they were designed to make efficient use of space and ensure that all of the equipment interconnected and functioned properly.[20] Likewise, the COs evolved over time, with equipment being placed where it made the most technical sense. COs were not, however, designed to accommodate or house equipment used by multiple carriers. For that reason, the CO building structure itself (*i.e.*, the exterior walls and doors of the premises) was the primary security measure to keep unauthorized individuals out.

Since the establishment of COs, circumstances have changed with the introduction of physical collocation. Physical collocation – and, in particular, cageless collocation or CCOE – inherently compromise Verizon MA's ability to protect its network *within* the CO.[21]

---

[20] For example, equipment with similar functions is grouped together; room for growth is planned for equipment, such as switches and frames, that must be contiguous; certain equipment (*e.g.*, power plant, circuit switches, interoffice and toll transmission equipment) may be segregated for technical and safety reasons; and infrastructure (*e.g.*, power, heating, ventilation, air conditioning, etc.) is designed to support each component. In addition, switches and transmission equipment are on different ground planes (*i.e.*, isolated versus integrated) and cannot be commingled for safety and personnel reasons.

[21] If new COs were built today, Verizon MA could design them with *interior* security in mind, and for example, place all of its sensitive equipment on one floor, and leave other parts of the CO with empty space for collocators. Verizon MA could also ensure that all the empty space in the CO was near a door that could be adequately secured.

Q. Please describe the effect of Verizon MA's network architecture on the types of security measures proposed.

A. Because of the critical and highly sensitive nature of the equipment located in Verizon MA's COs and the far-reaching effects of a network outage,[22] access to COs with physical collocation arrangements creates significant risks for Verizon MA and the end-user and carrier customers served by those COs. This is particularly true in COs with tandem switches, Signal Transfer Points ("STPs"), or emergency 911 ("E911") switches and adjunct equipment, each of which is critical to the network as they are used to complete interoffice and emergency calls. Although existing security measures, such as security cameras and badges with computerized tracking systems, may afford some protection, they alone cannot prevent damage to Verizon MA's network infrastructure.

Because of the design of COs, placing locked cabinets around Verizon MA's equipment and network is neither a technically feasible nor an economically viable option. Accordingly, to address these legitimate security concerns, Verizon MA should be permitted to apply a general policy of *secure* segregation and separation of its equipment areas and collocator equipment areas, and should be allowed to migrate physical collocation arrangements that do not comply with that standard. Contrary to the FCC conditions currently on appeal, Verizon MA

[22] Not only is inadvertent or intentional damage to the CO's operational and electronic equipment a concern, but also damage to its power plant and environmental support infrastructure (*e.g.*, water supply, heating, ventilation, and air conditioning system, etc) must be prevented.

should not be limited to requiring separate space only where no additional time or costs would be incurred. 47 C.F.R. §51.323(i)(4). The security risks to the network far outweigh these restrictions.

Currently, traditional "caged" physical collocation and SCOPE are provided in separate, secured areas of Verizon MA's COs. Likewise, all future physical collocation deployments must provide for such a secured arrangement. In those cases where new physical collocation arrangements cannot be provided in segregated CLEC areas with separate entrances, virtual collocation arrangements should be required.

Q. Please explain why Verizon MA believes the security risks raised by physical collocation can be best met by requiring separate rooms or segregated space – and providing a secured path or route to that space - for collocated carriers.

A. Verizon MA believes that a higher, yet reasonable, degree of security is required to ensure full network reliability, and can only be attained if collocators are located in separate and segregated areas of the CO. Providing a physical and secure barrier that prevents CLECs or others from gaining access to Verizon MA's CO equipment is necessary for several reasons.

First, while Verizon MA is permitted to escort its own vendors, the FCC and the Department require that Verizon MA provide a collocator with *unescorted* access to its equipment in the CO 24 hours a day, seven days a week. If Verizon MA is

not permitted to separate and secure that equipment, then non-Verizon employees will have unlimited access to the Company's network facilities, thereby increasing the risks of accidents and sabotage.

Second, Verizon MA requires that its own vendors adhere to the Company's "Safe Time" policy. This prohibits equipment installation or rearrangement activities within close proximity to working equipment except during late evening to early morning hours (*i.e.*, typically between 11:00 P.M. and 7:00 A.M.) when any accidental disruption to working equipment would have minimal impact on consumers. That safety policy would be undermined, and network security threatened, if separating or partitioning collocator equipment were not required, and collocator personnel could access unsecured equipment any time of the day.

Third, the number of collocators in Massachusetts COs range from one to as many as 27 CLECs per CO. Each CLEC, in turn, has many employees that would potentially have access to Verizon MA's COs. Even if Verizon employees are in the CO at the same time as the CLEC employees, they would not necessarily know which CLEC employees belonged in a particular CO and who did not (especially with the unauthorized sharing of identification badges and access cards), or on which piece of equipment a given technician was authorized to work. Physical separation of CLEC collocation equipment area and Verizon MA's equipment areas would provide Verizon MA with the ability to deter or prevent unauthorized individuals from venturing beyond their designated area into

areas where they have no reason or authority to access.[23] This provides further assurances that its network will be safer and better protected with higher and reasonably practical protection and.

Finally, placing CLEC equipment in a separate and secured area of the CO away from Verizon MA's equipment may also have the added benefit of providing not only superior, but often less expensive, security arrangements for both the Company and the collocator. This can allow easier access for the collocators' personnel and reduce the need for security cameras systems and other expensive security arrangements. Separate space that is dedicated to collocation can also be engineered with new collocation arrangements in mind, *e.g.*, to provide power and office connections likely to be requested by collocators. Provided that such space is not technically inferior to space elsewhere in the CO, Verizon MA should be permitted to require separate and secured space for all forms of physical collocation (including CCOE) to ensure the safety, security and reliability of the telecommunications network.[24]

Q. Please comment on the security concerns relating to the commingling of Verizon MA's and CLEC's equipment.

---

[23] Likewise, there are existing equipment areas in the CO where Verizon MA employees are restricted from entering, except for those employees who are properly trained to work on the equipment.

[24] It should be noted that the in its December 21, 2002, Brief on appeal, the FCC clarified its position, stating that separate rooms and entrances are permitted to address legitimate security concerns provided that the CLECs are not disadvantaged.

A. Commingling of Verizon MA's and CLEC's equipment in the same unpartitioned equipment area presents insurmountable security problems. Existing security measures, such as card readers, keys, and cameras, are simply not enough in a commingled environment absent secure partitioning, and would be cost prohibitive. Even if such security devices *could* be reasonably placed in all necessary areas in the CO, any accidental or intentional damage to Verizon MA's equipment would be exceptionally difficult to detect, much less prevent because of the close proximity of the CLEC equipment and CLEC personnel working on that equipment.

For example, video surveillance would be ineffective because when equipment is located in the same or adjacent bays, it is virtually impossible for an on-camera view to show on which piece of equipment a technician is working, let alone whether the technician has made inadvertent or intentional contact with equipment in an adjacent bay. Moreover, while video surveillance alone may provide some deterrent to interference with Verizon equipment, for the most part, it can only help determine accountability <u>after</u> the damage is done.

In addition, commingling raises considerable security risks because of the fundamental differences between Verizon MA's employees or vendors and CLEC employees or vendors, who would be installing and repairing equipment that is

not physically separate from the Company's equipment.[25] This is a key factor in permitting Verizon MA to require that CLEC equipment be separate and secure from the Company's equipment and not commingled. In addition, much of the equipment deployed by the CLECs looks the same as Verizon's equipment,[26] which increases the likelihood that CLEC personnel may inadvertently work on the wrong shelf - and directly or indirectly cause a service outage. Accordingly, Verizon MA should be allowed to require virtual collocation where available floor space limits preclude establishing a separate, segregated area for physical collocation.

---

[25] First, unlike Verizon's own employees, CLECs' employees are not accountable to Verizon. Verizon may escort a CLEC employee out of the CO if he/she is unauthorized or responsible for accidental or intentional damage in the CO. However, Verizon MA cannot terminate his/her employment, as it could its own employee or vendor. That distinction creates an incentive for Verizon MA's workforce and vendors to follow proper procedures and exercise care and caution when working around Verizon MA's equipment, and conversely a disincentive for CLEC employees or agents. In fact, the CLEC employee or agent can re-enter Verizon MA's CO at another time using someone else's access card, or may accompany a co-worker with a valid access card.

Second, Verizon MA has no way of knowing whether the CLEC employee has been adequately trained to work on equipment in a CO environment. Verizon's own employees undergo significant training before they are permitted to work in the CO, and some are even specifically trained and authorized to work on particular CO equipment, as noted above. Untrained CLEC employee/agent may accidentally damage Verizon MA's equipment while working on the CLEC's equipment, or may inadvertently work on Verizon MA's equipment in a commingled environment.

Finally, both because Verizon MA can carefully screen its employees and because Verizon MA is better able to hold its own employees and vendors accountable, physical segregation of CLEC equipment is preferred. This will minimize the likelihood that third parties, who have no legitimate business in Verizon's COs, will gain access to them.

[26] To the extent that CLEC and Verizon equipment may be the same, this also increases the likelihood that "spare parts" on hand in Verizon's CO will be "poached" if needed by a collocated carrier for provisioning or maintenance purposes, based on Verizon's actual experience nationwide in physically collocated COs. This too can result in service outages, as Verizon has experienced firsthand when CLECs have borrowed "in-use" Verizon equipment parts for their own needs, without Verizon's permission or prior knowledge

Q. What protections do CLECs have in a physical collocation environment?

A. CLECs already have adequate safeguards available to them to protect their equipment. Verizon MA provides "caged" physical collocation and SCOPE arrangement in separate collocation areas that are normally secured, with entry limited to collocators by means of magnetic coded cards, keys or keyed cipher locks. In addition, "caged" collocation provides for a wire mesh enclosure that surrounds the area allocated to the individual CLEC. That cage is provisioned with a locking door to which the CLEC has the key.

CLECs opting for additional security can request installation of tops on their physical cages, or may elect to install locking cabinets or covers for their equipment in caged or cageless collocation arrangements. Similar security arrangements for Verizon MA's equipment would not be possible if separate space was not required and commingling of equipment was permitted.

Q. Please explain the security concerns raised by cageless collocation, and Verizon MA's proposed security measures to address those concerns.

A. Cageless collocation or CCOE differs from "caged" physical collocation and SCOPE in that it does not require the establishment of separate space for the collocated carrier. Indeed, CCOE is used where *separate* physical collocation space is not available due to space restrictions in a particular CO. In fact, some existing CCOE arrangements in Massachusetts are *unsecured*, which means that

they are located in areas where Verizon MA's equipment is already placed and cannot be segregated. This configuration presents serious security concerns.

It is virtually impossible to provide adequate security for Verizon MA's facilities in an unsecured environment where CLEC personnel is allowed 24 hour a day, seven days a week unescorted access. Such conditions lead to increased potential opportunities for accidental or intentional dislodging of Verizon MA's connections or damage to other Company equipment that is exposed and physically unseparated from collocators' equipment. Verizon MA must be able to protect its own equipment without having to resort to massive reconstruction and reengineering. Placing locked cabinets around Verizon MA's equipment is not technically or operationally feasible without moving equipment to make space for such cabinets and without reconstructing the entire heating, ventilation, and air conditioning system in its COs. In addition, even if this were technically feasible, it would not be practicable because of the amount of available space in most Verizon MA COs.

Verizon MA estimates that approximately 13 of the 27 CCOE arrangements in Massachusetts are placed in unsecured areas within nine COs. Because unsecured CCOE arrangements pose unacceptable and unnecessary risks to the security and reliability of Verizon MA's network, the Company recommends that, in those limited instances, the existing arrangements must either be rearranged to a

segregated collocated area within the CO or converted to virtual collocation, in place if feasible.

Likewise, to ensure that network safety and reliability is maintained, Verizon MA proposes that future CCOE arrangements only be placed in separate and secured collocation areas. This approach is not only warranted for security reasons, but is consistent with the *FCC Remand Order*, which expanded Verizon MA's rights to separate and segregate physically collocated equipment within its premises.

Q. How does Verizon MA propose to address security issues raised by collocated carriers' need for reasonable access to shared facilitiesin the CO?

A. The FCC has found that collocated carriers are entitled to reasonable access to shared facilities (*e.g.*, temporary staging areas, loading docks, restrooms, and elevators) in Verizon MA's COs. *FCC Advanced Services Order* at ¶ 49. In some COs, this means that CLECs must traverse areas where Verizon MA's equipment is located to access these shared facilities. Thus, while physical collocation arrangements may be separate and secure, access to shared facilitiesis not. For security reasons, access to shared facilities also needs to be limited to where these facilities can only be accessed *without* entry to Verizon MA's equipment areas.

Verizon MA has not quantified how many COs with physical collocation do <u>not</u> have a physically secured passage or access to shared facilitiesseparated from

Verizon's equipment space.[27] However, Verizon MA proposes to determine where partitioning is feasible to protect Verizon MA's network from inadvertent or deliberate harm while providing collocators with "reasonable access" to common areas. In those COs where such partitioning is not feasible, CLEC access to other areas outside of the existing physical collocation arrangements is not required, and should not be permitted. Verizon MA will, however, continue to coordinate, at the carrier's expense, pre-arranged access to certain common areas, such as temporary staging areas and loading docks, for the delivery and unpacking of collocated carriers' equipment for a given CO. This is the only reasonable and effective means of providing adequate network security in a collocated environment where separate space or physical barriers cannot be erected to segregate, secure and protect Verizon MA's equipment.

Q. Please describe the security concerns raised by CRTEE arrangements, and Verizon MA's proposed security measures to address those concerns.

A. Verizon MA offers CRTEE in accordance with the FCC's collocation requirements. The FCC is currently reviewing the appropriate security measures for such arrangements in connection with its *Remand Order*. *FCC Reconsideration Order* at ¶ 104. Although no CRTEE arrangements currently exist in Massachusetts, Verizon MA believes that the Department should address

[27] In most smaller COs, this basically means that collocators have unfettered access to roam about the CO.

the unique security problems raised by RTs in this proceeding in the event that CRTEE is requested by a CLEC in the future.

As explained in Attachment 3, RTs are freestanding structures (e.g., CEVs, huts or cabinets) located outside of the CO that house telecommunications electronic equipment. Because RTs house much of the same costly and delicate equipment housed in a CO, they present the same opportunities for service disruption, equipment tampering and theft, as discussed above. However, securing RTs is even more problematic because of their extremely small size and their location.

There are more than 2000 RT structures in Massachusetts. Inadvertent or improper actions within the tightly engineered and confined space of RT can cause service disruptions for many customers. Customers served through RTs would be as isolated from critical emergency services and other communications just as if the damage originated in the CO. However, because redundant network facilities in an RT are more closely located with other facilities, the likelihood of service-affecting consequences is even greater than in the CO.

Unlike a CO, in most cases, it would be practically impossible to segregate Verizon MA's equipment into separate space in an RT. As explained in Attachment 3, none of the RT structures is designed to enable Verizon MA to secure its equipment, as well as power, from access by other carriers. For example, CEVs and huts are sized so that a technician can enter the enclosure and gain access to the equipment and wiring in the limited space available. RT

structures typically have no space for more than one or two individuals, at most, at one time. Partitioning or securing equipment inside a locked enclosure inside the small RT is, therefore, not a practical solution because of the additional space such an enclosure would occupy and the lack of excess space in the confined RT structure.

Likewise, providing secure access to RT locations would become an increasingly difficult problem to administer and control. Access to the various types of RTs include padlocks, keys and special tools. Retrofitting RTs for other security mechanisms (*e.g.*, placing card readers or cameras) to give other carriers access would be a significant and costly undertaking. This also assumes that those methods alone would provide adequate network security – which they would not, for the reasons discussed above. The only way to ensure adequate security at an RT is to allow Verizon MA to limit RTs to virtual collocation or, in the alternative, to require a security escort for the CLEC technicians.

Virtual collocation will enable Verizon MA to reasonably protect its equipment because only Company technicians would be allowed to install and maintain equipment that the collocated carriers supply. This would make more efficient use of the limited available space because it eliminates the need to segregate equipment within the RT. It would also prevent one carrier's collocated equipment from being inadvertently affected by another carrier's technician working in the limited space. In addition, Verizon technicians are properly

trained on taking necessary precautions in entering CEVs, which must be properly ventilated and checked for foreign, gaseous odors prior to entering the structure.

If, however, the Department does require physical collocation at RTs, which it should not, then the only practical means of protecting Verizon MA's network facilities is to require the use of escorts to accompany collocators that *maintain* their own equipment. Because of the greater possibility of accidental or intentional damage, collocators should not, however, be permitted to install their own equipment in RTs, even under a physical collocation arrangement.

Q. How does allowing CLEC access to manholes present increased security concerns?

A. As part of the FCC's collocation requirements, CLECs may have access to Verizon MA's manholes in deploying their own fiber optic entrance cable.[28] Verizon MA's manholes are used access to underground inter-office and feeder/distribution facilities, and are often small, dark and densely filled. Because the cramped working area increases the potential for damaging other proximate network facilities, Verizon MA requires the presence of a Contract Work Inspector ("CWI") when CLECs require access to manholes to place facilities. Applicable terms and conditions are contained in Verizon's standard conduit

[28] *Local Competition Order*, at ¶ 1119; *see also* 47 U.S.C. § 251(b)(4) (citing LEC's "duty to afford access to the poles, ducts, conduits, and rights-of-way of such carrier to competing providers of telecommunications services on rates, terms, and conditions that are consistent with section 224" of the Telecommunications Act of 1996).

occupancy agreement, which must be executed by a CLEC prior to placing its facilities in Verizon MA's conduit systems. Although Verizon MA has experienced some CLEC violations of these security practices, the Company proposes no change in its current practices at this time.

Q. Please comment on Verizon MA's proposal to classify certain select COs as "critical" sites that would provide virtual collocation only, even if physical collocation space were otherwise available.

A. Verizon MA proposes to work with the Department to identify those "critical" COs where virtual collocation only should be required. The key factors to consider in determining the critical nature of a central office may include: (1) the type of switch or signaling elements housed in a CO; (2) the presence of critical customers (*e.g.*, major airport, military installation, government agencies, and/or nuclear power plant) served by a CO; and (3) the number of access lines and special services circuits served by a CO. For example, a CO may be more critical if it houses a tandem switch, an E911 tandem switch, and/or STP equipment that are the "lifeline" to numerous subtending switches throughout Massachusetts.

Accidental or intentional damage to the network resulting in disruption of existing service in those particular COs could pose national security risks, endanger the health, safety and welfare of many more lives, and jeopardize the operations of major businesses, public safety, and government agencies, as well as advanced technology companies and other institutions that are involved in national security

matters. Therefore, the security and network reliability of Verizon's infrastructure in serving those select COs would be of national importance.

Based on this preliminary criteria, there is a handful of Massachusetts COs that would meet this criteria and be designated as "critical," providing *only* for virtual collocation arrangements for security reasons. Verizon MA would recommend that any existing physical collocation arrangements in those critical COs be converted to virtual collocation arrangements. Where feasible, physical collocation would be converted to virtual "in place," thereby minimizing any added security costs borne by the CLECs.

COST RECOVERY PRINCIPLES

Q. Who should bear the costs associated with enhanced security measures in Verizon MA's physically collocated COs or RTs?

A. While Verizon MA has not determined the costs associated with its proposed collocation security plan,[29] the Company believes that it should be permitted to recover those costs from the cost-causer, *i.e.*, the collocated carriers. To the extent that conversions of existing physical collocation arrangements to virtual collocation are required under the terms and conditions as described above,

[29] "Reasonable security costs" related to collocation and recoverable from the CLECs may include the costs of standard security devices, such as electronic card readers, security cameras, etc., as well as the costs associated with the construction of new walls, structures, or entrances for separate space and/or the use of escorts.

Verizon MA will endeavor to transfer those arrangements "in-place," thereby minimizing the costs passed on to the CLECs.

Allowing Verizon MA to recover its additional security-related costs from the collocated carriers is fully consistent with the longstanding economic cost recovery principle of cost causation. As previously explained, COs and RTs were originally designed to protect the equipment from within, meaning that the facilities were locked and only authorized Company employees were permitted access to those sites. However, with physical collocation, multiple carriers' equipment is now placed in Verizon MA's CO, and many more individuals are allowed access to Verizon MA's facilities.

For example, in Massachusetts alone, there are 46 CLECs who have currently have 948 physical collocation arrangements and 4 virtual collocation arrangements in 169 Verizon MA COs. This influx of "foot traffic" in the CO dramatically increases the security risks to the network infrastructure and directly affects the type of security measures that can and must be imposed. Those same security methods would not otherwise be required if Verizon MA were the only carrier occupying the CO space. Accordingly, because the collocated carriers benefit from access to Verizon MA's COs and RTs, and reasonably cause the added security costs to be incurred, they – not Verizon MA – should bear the full costs associated with the additional security measures taken to protect the network from harm.

Q. Does this conclude Verizon MA's testimony?

A. Yes.